

# DMVPN LAB

## 1. Preparation questions:

- a. What is the GRE tunneling protocol? How does it differ from other IP based tunneling protocols such as L2TP and IPsec?
- b. Give a short explanation about IPsec protocol.
- c. what are the key components of DMVPN?
- d. How many phases does the Dynamic Multipoint Virtual Private Network (DMVPN) protocol have, and what are the characteristics of each phase?
- e. what is the difference between DMVPN and GRE + IPSEC pros&cons between them?
- f. How does DMVPN enhance the scalability and flexibility of VPN deployments in enterprise networks?
- g. How do dynamic routing protocols like EIGRP, OSPF, or BGP integrate with DMVPN to improve network efficiency?
- h. What security mechanisms are used in DMVPN tunnels and the DMVPN protocol overall?
- i. What is EIGRP protocol? How does it differ from OSPF/BGP and what are the uses of the protocol?
- j. What is NHRP protocol? How is important to DMVPN protocol?
- k. Explain what is mGRE, what is the benefit of using it against GRE?

## Recommended Links:

- dynamic multipoint VPN (DMVPN):  
[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html)  
<https://nordvpn.com/he/blog/dynamic-multipoint-vpn/>
- DMVPN over IPsec:  
<https://networklessons.com/cisco/ccie-routing-switching/dmvpn-over-ipsec>
- Configuring DMVPN:  
<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dmvpn.html>
- Enhanced Interior Gateway Routing Protocol  
[https://en.wikipedia.org/wiki/Enhanced\\_Interior\\_Gateway\\_Routing\\_Protocol#:~:text=EIGRP%20is%20used%20on%20a,that%20needs%20to%20be%20transmitted.](https://en.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol#:~:text=EIGRP%20is%20used%20on%20a,that%20needs%20to%20be%20transmitted.)
- NHRP protocol:  
[https://www.techtarget.com/searchnetworking/definition/Next-Hop-Resolution-Protocol#:~:text=Next%20Hop%20Resolution%20Protocol%20\(NHRP\)%20is%20an%20automated%20configuration%20technology,%2D%2D%20to%20the%20receiving%20computer](https://www.techtarget.com/searchnetworking/definition/Next-Hop-Resolution-Protocol#:~:text=Next%20Hop%20Resolution%20Protocol%20(NHRP)%20is%20an%20automated%20configuration%20technology,%2D%2D%20to%20the%20receiving%20computer)
- mGRE:  
<https://www.cbttuggets.com/blog/technology/networking/what-is-a-gre-multipoint-tunnel>

# DMVPN LAB

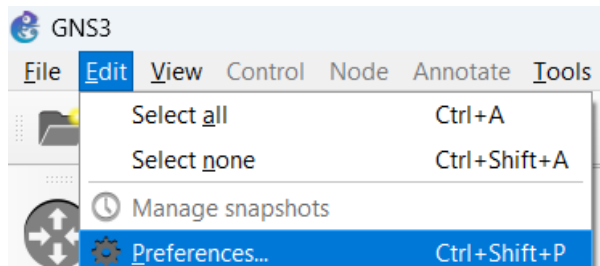
## Pre requirements –

- windows 10 or windows 11.
- GNS3 installed on PC.
- Intel CPU that supports intel virtualization technology – you are able to search your CPU in Intel site and check if it is support this technology. Here a short guide that explains how to do so - <https://www.intel.com/content/www/us/en/support/articles/000005486/processors.html>

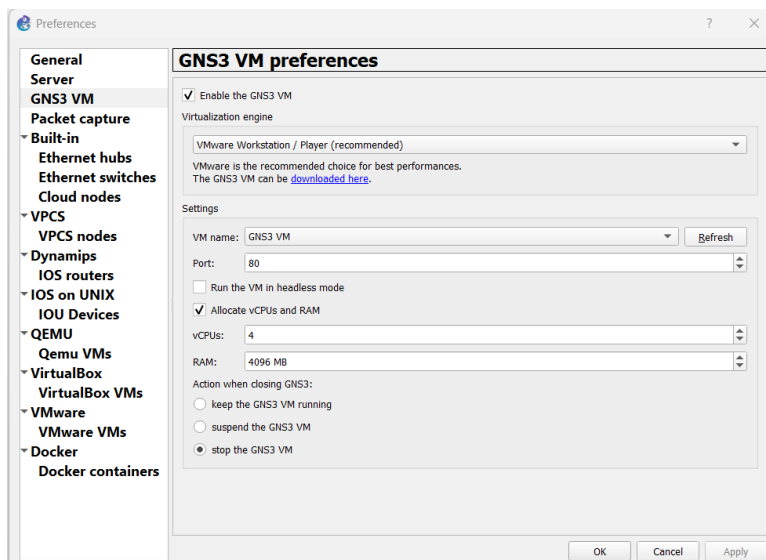
## 2. Section material:

In order to do this lab you need to download and install the following items:

- a. **GNS VM** – It is fully recommended to install routers and switches (or any GNS appliance) over the GNS VM. In order to install the GNS VM do those steps – for this lab it is necessary to install GNS VM.
  - Download the GNS3 VM from this website, **pay attention that your GNS3 version and GNS VM version are the same** - <https://gns3.com/software/download-vm>
  - GNS recommended to install the GNS VM on the VMware instead of VirtualBox. Download VMware Workstation player or VMware Workstation Pro from this website (Player is free version) - <https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html.html.html.html>
  - After both installed, right click on GNS VM.ova file, click on “open with” and click on VMware player. Choose name and install the VM over the VMware.
  - Close VMware (if open) and open GNS3. Click on edit tab -> preferences.



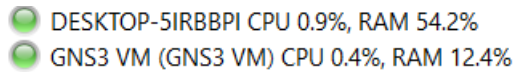
- Tick enable GNS VM, and use VMware Virtual machine you just installed. Set the settings as the photo below:



# DMVPN LAB

**Pay attention – if you want to change the vCPUs number or RAM, change in the GNS settings and not in the VMware settings.** We recommend at least on 4 CPUs and 4096 MB of RAM.

- Reopen GNS3, do not open new project just wait till both servers status are online (green mode). Here a photo that represent that status:



it is normal that when GNS3 is open the GNS VM is open as well, this is the VM itself.

- **Possible problems** – When you finish the steps above, make sure that the GNS VM status is as follows –
  - i. There are IP and port
  - ii. There are SSH details
  - iii. There is WEB-UI
  - iv. Most important – KVM support available is True.

```
GNS3 server version: 2.2.47
Release channel: 2.2
VM version: 0.16.0
Ubuntu version: focal
Qemu version: 4.2.1
Virtualization: vmware
KVM support available: True
Uptime: up 0 minutes

IP: 192.168.244.128 PORT: 80

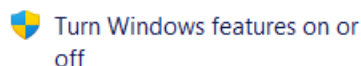
To log in using SSH: ssh gns3@192.168.244.128
Password: gns3

To launch the Web-Ui: http://192.168.244.128

Images and projects are stored in '/opt/gns3'
```

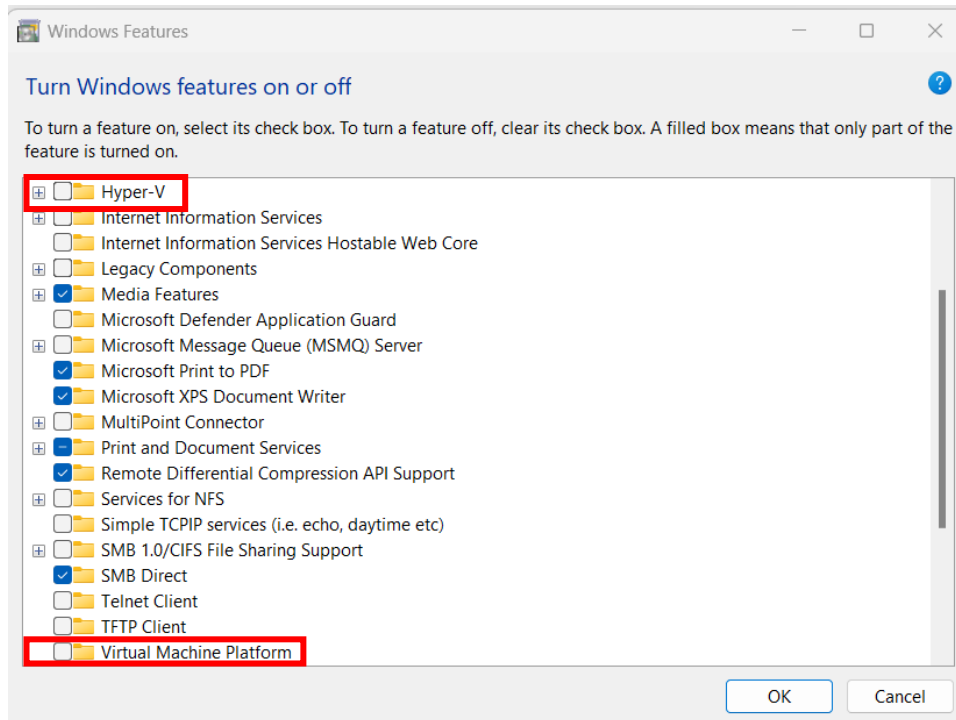
It is very common that KVM support available will be False, in order to fix that do these steps:

- i. Make sure the firewall is off.
- ii. Go to control panel -> Programs and Features -> Turn windows features off or on.

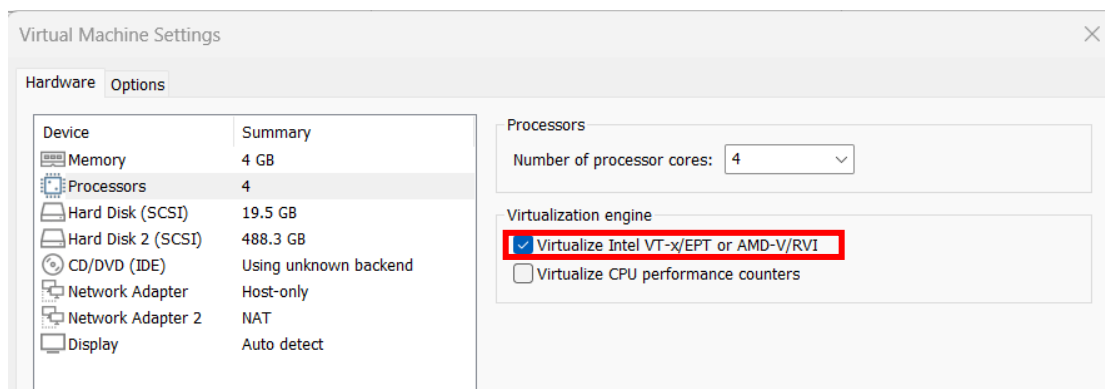


- iii. Make sure Hyper-V and virtual machine platform are unticked.

# DMVPN LAB








- iv. Open VMware player, right click on the GNS VM, choose settings and go under processors. Make sure Intel VT-x is ticked.



- v. Turn off the pc, and turn it on. while the pc is booting click on f2 bottom on the key board (long click). The pc will enter to BIOS mode. Go to BIOS settings and look for Intel VT-x or Intel Virtualize technology, make sure this option is enabled.
- vi. Restart PC and reload GNS, wait for both servers to be online and make sure KVM support available is True.

# DMVPN LAB

b. **GNS Appliances** – for this lab you have to install specific cisco router and switch. In addition you will have to install ubuntu docker.

- Download the Cisco router from this link - <https://upw.io/4zu/vios-adventerprise9-m.vmdk.SPA.156-2.T.qcow2>
- Download the Cisco switch from this link - [https://upw.io/75f/vios\\_l2-adventerprise9-m.SSA.high\\_iron\\_20180619.qcow2](https://upw.io/75f/vios_l2-adventerprise9-m.SSA.high_iron_20180619.qcow2)
- 
- Open GNS3 (wait both servers, local and VM are online), click on routers button  and then click on new template –  New template
- Click “Install an appliance from the GNS3 server (recommended).
- Search under Routers Cisco IOSv-  Cisco IOSv -> install.
- Click on “Install the appliance on the GNS3 VM (recommended).  
**Make sure the GNS VM is online.**
- Keep the path in the Qemu binary phase as default.
- Look for IOSv version 15.6(2)T and expend it.
- Click on vios-adventerprise9-m.vmdk.SPA.156-2.T and than click import button.
- Search the Router file you downloaded from the beginning of this section and choose it.
- Make sure now its status changed to “Found on GNS3 VM”.
- Click on IOSv\_startup\_config.img and click on download button (it will open new site, download the file and than import it.
- Now you should be able to install this router.
- Click install and finish the installation of the router.
- Now let’s do the process again – click on switched button  and click on new template button.
- Do just the same as the router installation process except three changes:
  - i. Make sure you search this time under switcher – Cisco IOSvL2 switch.
  - ii. Look for IOSvL2 version 15.2.1
  - iii. Make sure you import the switch file you download in the beginning of this section.
- Now let’s click on PC’s icon  click on new template, and Click on “Install the appliance on the GNS3 VM (recommended).
- Search under guests after ubuntu docker guest.
- Install on GNS VM as before and finish installation.
- Right click on the the PC and click on “configure template”.
- Click on Browse button -

Symbol:

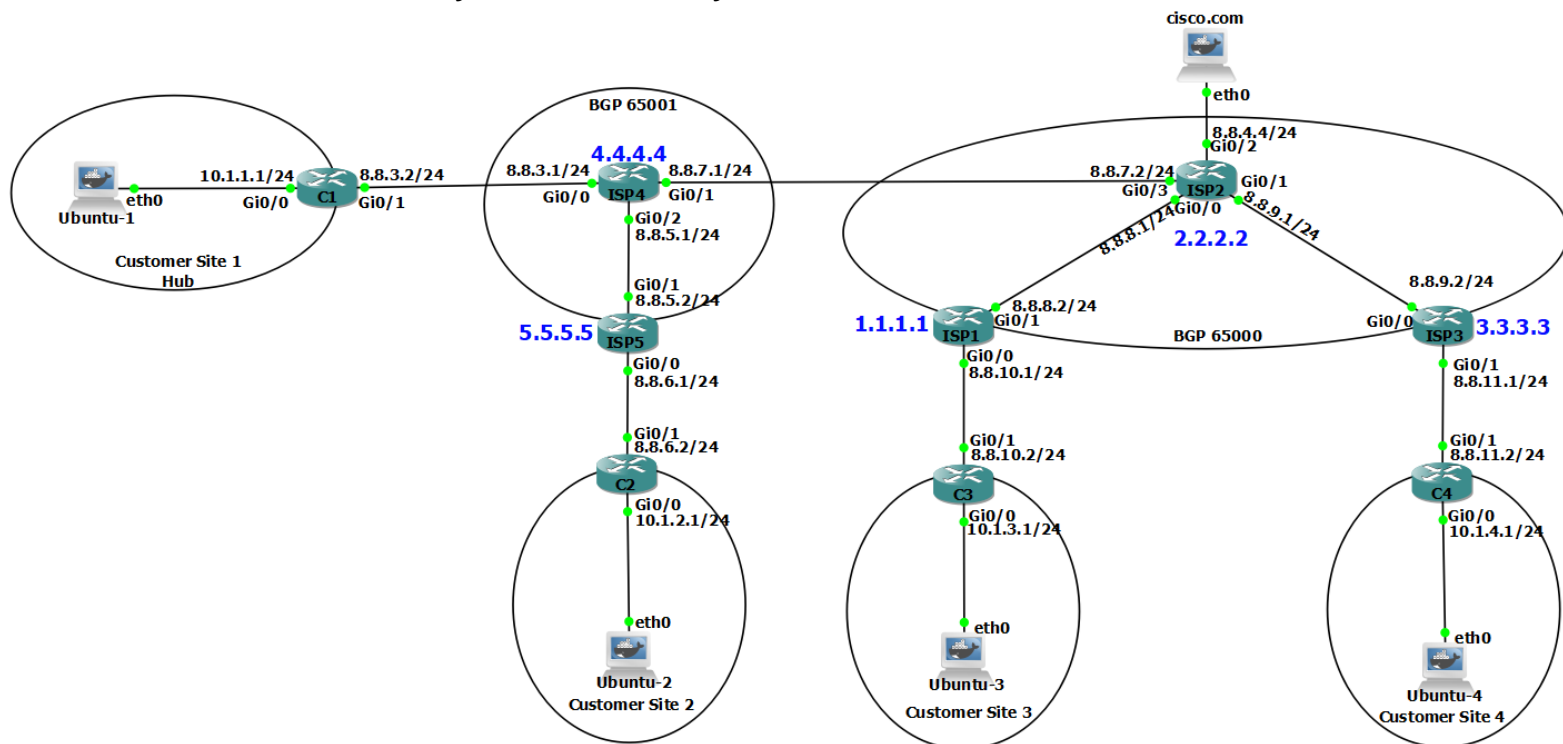
And search after docker\_guest under classic section.

- Click ok.

**The installation process is finished.**

# DMVPN LAB

3. This is GNS3 topology that consists of multiple protocols. And you need to configure two version of dynamics multi-point VPNs. You firstly configure a full mesh DMVPN using GRE without encryption and once you've got that working you need to enable IPSEC encryption for your VPN tunnel.
4. The lab emulates a topology as shown below. Customer router 1 will be the hub, customer 2-4 are spoke sites. Create topology as described below. Where the addresses marked in blue are loopback addresses, and the rest are the networks for the interfaces ip addresses. Make sure all loopbacks and interfaces are configured. Full mesh DMVPN will be configured during the lab using BGP, DHCP, IPSEC, EIGRP, mGRE and NAT. **Don't forget to run the routers one-by-one (not all together) while monitoring RAM usage of GNS VM server by Servers Summary.**



In order to configure the cisco.com PC, enter to pc console and use “nano /etc/network/interfaces”, make sure the configurations look the same:

```
#
# This is a sample network config uncomment lines to configure the network
#

# Static config for eth0
auto eth0
iface eth0 inet static
    address 8.8.4.8
    netmask 255.255.255.0
    gateway 8.8.4.4
    up echo nameserver 8.8.4.4 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
```

In addition – use nano /etc/resolv.conf and make sure it looks like this (DNS USES):

```
nameserver 8.8.4.4
```

# DMVPN LAB

5. **Routing Protocols** - The first part of the lab is to configure routing protocols in ISP networks:

## BGP

- a. Let's start with ISP4 and ISP5 Use the command "ip protocol" in order to display the routing protocol that configure to the router (if any). Add a snapshot of the result.
- b. Configure iBGP neighbor relationship between ISP4 and ISP5. add a screenshot of the BGP table of each router, use "show ip bgp" command. Make sure the BGP configuration is for the same AS 65001.
- c. Configure eBGP from ISP4 to ISP2 (remember to use the correct As, this time they don't have the same AS IPS2 is under AS 65000). use "show ip bgp sum", what is the current state of the BGP relationship and why? Explain each field in the table.
- d. Configure eBGP between ISP4 and ISP2 from ISP2 router this time.
- e. Provide results of "show run | section bgp" and "show ip bgp sum", explain the results, make sure 5 networks on the router and 3 network relationships and that the ISP4 – ISP2 state is now active and not idle anymore.
- f. Don't forget when you configure ISP2, add ISP1 and ISP3 as neighbors in the same AS (65000).
- g. Try to ping ISP5 from ISP2 – ad screenshot of the results.
- h. **Do not configure BGP between ISP2 and ISP1/ISP3 physical interfaces, instead configure between ISP2 and ISP1/ISP3 loopbacks only!**
- i. In order do configure BGP using loopbacks in addition to the "area-as" command we used, use "update-source" command. (full command under configurations section in the end of the lab). Use this command in ISP2 for ISP1 and ISP3 loopbacks.
- j. Configure ISP1 and ISP3, advertise the networks, assign as neighbor the ISP2 loopback only.

## IGP - OSPF

- k. Configure IGP (OSPF) at ISP1 and ISP3 only to the ISP network (do not enable OSPF towards the costumers).
- l. Configure ISP2 with OSPF on the other side of the ISP1/ISP3 links and loopbacks.
- m. Make sure you are able to ping IPS1/IPS3 to IPS4/IPS5.  
In this phase we are not configuring BGP between ISP1 and ISP3 directly. We will do it later. **Why we need to do so?**

6. **DHCP pools on the ubuntu clients –**

- a. We will start with router C1 (DHCP router of costumer 1). First, check with "show ip brief" the ip addresses that configured in the router. Make sure everything is configured like the topology provided above.
- b. Make sure C1 (the DHCP router) doesn't allocate IP addresses between 10.1.1.1 to 10.1.1.10. it shouldn't but sometime it does. Use "excluded-address" in order to do so (full explanation in the table at the bottom of the lab).

# DMVPN LAB

- c. Create DHCP pool to the network. Make sure C1 ip is the default router.
- d. Use google 8.8.8.8 as DNS-server.
- e. Show DHCP binding with "show ip dhcp binding" and add to the report.
- f. Try to ping to the PC address.
- g. Go to the PC command, use "ifconfig" and make sure the new IP is shown. Add a screenshot.
- h. Do the same process for all DHCP servers of the costumers.
- i. Remember to configure the Ubuntu PC docker to support DHCP server. In order to do so edit (with nano or any other program), etc/network/interfaces and remove the # sign before the "auto eth0" line and "iface eth0 inet dhcp" line. Save the interfaces file and reboot the PC.
- j. To make sure everything works, try to ping between each costumer and its DHCP server.

## **7. DMVPN (Using EIGRP, mGRE and NHRP) –**

- a. Start a Wireshark capture on the link between C1 and ISP4 and on one of the branch interfaces (e.g link between C2 and ISP5).
- b. Configure costumer site 1 as the hub of the DMVPN and costumer site 2 as the spokes.
  - In order to do so, do the following: (configuration commands describes in the end of the lab file)
  - Create a tunnel using 192.168.1.X as IP (X = 1,2,3,4 respectively to c1, c2, c3, c4).
  - Configure NHRP
  - Configure mGRE.
  - Configure EIGRP

Don't forget to configure static default to each router (hub or spoke)

- c. Add the result of the "show ip int brief" command and check if new IP is added to the table? If yes – who so?
- d. This time configure C2 with DMVPN as costumer
- e. Check in C2 if new IP is added to it table.
- f. Use "show dmvpn" command, add a photo of the table and explain each field.
- g. Try to ping to 8.8.3.2 – does it work? Explain?
- h. Add static default route to the hub and the costumers.
- i. does the ping work now? Add a screen shot.
- j. Use "ip eigrp neighbors" and add a screenshot of the table.
- k. Check the ISP routers, pay attention – they never learnt about network 10.0.0.0 or 192.0.0.0. so how the connection between C1 and C2 works?
- l. This time try to ping between Ubuntu1 pc and Ubuntu 2 pc – does it work?
- m. With Wireshark analyze the NHRP packets and their contents.
- n. In C1 (hub router) user "Show ip route", there is way to know that the network between C1 and C2 is via tunnel? Add a photo.
- o. Configure C3, and C4 as spokes in the same manner.
- p. After finished configuring C3 and C4 (and ping to C1 is work), use "show dmvpn". Only one record in the table, ping to C2 and add the new table results.
- q. Does the tunnel between C4 and C3 works? Why so?



# DMVPN LAB

- r. Configure BGP between ISP1 and ISP3.
- s. Explain why the BGP configuration was important for the tunnel to work?

## 8. NAT –

- a. At this phase we are able to ping from ubuntu1 to ubuntu 2,3 and 4. We want to be able to ping cisco.com as well. Try to ping to 8.8.7.1, it shouldn't work, why?
- b. Configure NAT on C1 when g0/1 is outside interface and g0/0 inside interface.
- c. Use show ip nat translations, now ping from ubuntu 1 to 8.8.7.1, it works now?
- d. Use show ip nat translations again, the output changed? Keep it.
- e. Try to ping to ubuntu 2 now, use show ip nat translations again, does the GRE appears on the table?
- f. This time ping to cisco.com (if it doesn't work reboot the ubuntu PC, sometimes the network established before the dns record is added to the pc, restart helps).
- g. Repeat the process on C2,C3 and C4.

## 9. IPSEC (DMVPN security) –

In order to make the DMVPN tunnel to be security, lets configure IPSEC and make security DMVPN.

- a. First, capture the traffic between ISP4 and ISP2. Try to locate EIGRP packets, does it readable?
- b. Keep capturing, ping from Ubuntu 1 to Ubuntu 4 , does the ICMP packets are readable?
- c. Configure IPSEC in C1.
- d. You may be able that there are no EIGRP neighbors anymore, why?
- e. Use "show crypto ipsec sa", pay attention for each costumer there is a paragraph. How many packets sent for each costumer? Why?
- f. Use "show crypto isakmp sa". There are deletions? Why?
- g. Configure ipsec for C2, C3 and C4.
- h. Use "show crypto isakmp sa". There are deletions now? Add a photo?
- i. Ping from ubuntu1 to ubuntu 4 and keep capturing the link between ISP2 and ISP4. There are EIGRP or ICMP packets now? Why?
- j. Are you able to find ESP packets?
- k. From ubuntu 1, ping to ubuntu 4 and ping to ubuntu cisco.com, there is an ICMP packet for ubuntu cisco.com? why so?

## 10. Discussion –

- a. Can a DMVPN network be set up with multiple hubs? If so, explain the rationale and provide at least two reasons for doing so. If not, explain why it cannot be done.
- b. What is the purpose of configuring the #ip nhrp map multicast ?
- c. What is the necessity of using a dynamic routing protocol within the tunnel network?
- d. IPsec typically does not support multicast messages. Why is it functioning in this scenario?

# DMVPN LAB

## Part 1 – BGP and IGP

step	Command or Action Purpose	Purpose
BGP	ID(config)#router bgp bgp_AS_num	Configure bgp
	ID (config-router)#neighbor ip_addr remote-as bgp_AS_num	set up a BGP session
	ID (config-router)#network ip_addr mask net_mask	When ip_addr and net_mask is the address to advertise
	ID (config-router)#neighbor loopback_ip update-source loopback 0	specify which interface IP address the router should use as the source IP address
OSPF	ID(config)#router ospf ospf_area	Configure ospf
	ID (config-router)#network ip_addr mask area ospf_area	set up a ospf session

## Part 2 –DHCP

step	Command or Action Purpose	Purpose
DHCP	ID(config)#ip dhcp excluded-address from_ip to_ip	This line commands to the DHCP server to do not allocate IP addresses between “from_ip” to “to_ip range.
	Ip dhcp pool name_dhcp	This command defines a new DHCP pool, which is a set of IP addresses that can be assigned to DHCP clients.
	Network ip_addr mask	This command specifies the network and subnet mask for the DHCP pool, defining the range of IP addresses that can be assigned to clients.
	Default-router ip_addr	This command sets the default gateway IP address for the DHCP clients. The default gateway is the IP address of the router that the clients will use to access other networks.
	Dns-server dns_ip	This command specifies the DNS server IP address that will be assigned to the DHCP clients. The DNS server resolves domain names to IP addresses.

## Part 3 –DMVPN –

step	Command or Action Purpose	Purpose
<b>Configure Hub</b>		
Tunnle and NHRP	interface Tunnel tunnel_number	This command creates a tunnel interface with the identifier tunnel_number
	ip address 192.168.1.X ip_mask	Sets the IP address and subnet mask for the tunnel interface.
	bandwidth bw_number	Sets the bandwidth for the interface to bw_number kbps (used by routing protocols for metric calculations).
	delay delay_number	Sets the delay_number value for the interface in tens of microseconds (used by routing protocols for metric calculations).
	ip nhrp holdtime 360	Specifies the NHRP (Next Hop Resolution Protocol) hold time in seconds. This determines how long NHRP mappings are kept.
	ip nhrp network-id 10000Y	Assigns a unique network ID to the NHRP domain. This ID is used to differentiate between different NHRP networks Use Y as your pair number
	ip nhrp authentication cisco	Enables NHRP authentication using the key <code>cisco</code> . This provides an extra layer of security for NHRP communications.
	ip mtu 1400	Sets the Maximum Transmission Unit (MTU) size to 1400 bytes for the interface to avoid fragmentation issues.
	ip tcp adjust-mss 1360	Adjusts the Maximum Segment Size (MSS) for TCP packets going through the tunnel to avoid fragmentation due to the lower

# DMVPN LAB

		MTU.
	ip nhrp map multicast dynamic	Enables dynamic mapping of multicast traffic. This allows NHRP to automatically map multicast traffic to the appropriate physical IP addresses dynamically learned through NHRP.
	tunnel source interface_num	Specifies the physical interface (interface_num) as the source of the tunnel.
	no ip split-horizon eigrp 100	Disables the split-horizon rule for EIGRP on this interface. Split-horizon is a technique to prevent routing loops by prohibiting a router from advertising a route back out of the interface from which it was learned. Disabling this allows the hub to advertise routes learned from one spoke to another spoke.
	no ip next-hop-self eigrp 100	Disables the next-hop-self feature for EIGRP on this interface. Normally, a router would set itself as the next-hop for routes it advertises. Disabling this allows the actual next-hop addresses to be preserved, which is useful in a hub-and-spoke topology where spokes should see each other as next hops.
mGRE	tunnel mode gre multipoint	Sets the tunnel mode to GRE (Generic Routing Encapsulation) multipoint. This is required for DMVPN to allow multiple spokes to communicate with each other through the hub.
	tunnel key 10000Y	Sets the key for the GRE tunnel, which is used to differentiate between different GRE tunnels.
EIGRP	router eigrp AS_NUM	Starts the EIGRP (Enhanced Interior Gateway Routing Protocol) process with Autonomous System (AS) number AS_NUM.
	network 192.168.1.X 0.0.0.0	Advertises the 192.168.1.X/32 network in EIGRP.
	network 10.0.0.0 0.255.255.255	Advertises the 10.0.0.0 network in EIGRP.
	no auto-summary	Disables automatic summarization of networks at major network boundaries.
<b>Configure Spoke</b>		
Tunnle and NHRP	interface Tunnel tunnel_number	This command creates a tunnel interface with the identifier tunnel_number
	ip address 192.168.1.X ip_mask	Sets the IP address and subnet mask for the tunnel interface.
	bandwidth bw_number	Sets the bandwidth for the interface to bw_number kbps (used by routing protocols for metric calculations).
	delay delay_number	Sets the delay_number value for the interface in tens of microseconds (used by routing protocols for metric calculations).
	ip nhrp holdtime 360	Specifies the NHRP (Next Hop Resolution Protocol) hold time in seconds. This determines how long NHRP mappings are kept.
	ip nhrp network-id 10000Y	Assigns a unique network ID to the NHRP domain. This ID is used to differentiate between different NHRP networks Use Y as your pair number
	ip nhrp authentication cisco	Enables NHRP authentication using the key cisco. This provides an extra layer of security for NHRP communications.
	ip mtu 1400	Sets the Maximum Transmission Unit (MTU) size to 1400 bytes for the interface to avoid fragmentation issues.
	ip tcp adjust-mss 1360	Adjusts the Maximum Segment Size (MSS) for TCP packets going through the tunnel to avoid fragmentation due to the lower MTU.
	ip nhrp nhs hub_address	Configures the Next Hop Server (NHS) IP address. This is the hub's address in the DMVPN network.
	ip nhrp map multicast ip_addr	Maps the multicast traffic to the physical IP address ip_addr. This allows multicast traffic to traverse the DMVPN network.
	ip nhrp map tunnel_ip physical_ip	Maps the tunnel IP address tunnel_ip to the physical IP address physical_ip This creates a static mapping for NHRP.

# DMVPN LAB

	tunnel source interface_num	Specifies the physical interface (interface_num) as the source of the tunnel.
mGRE	tunnel mode gre multipoint	Sets the tunnel mode to GRE (Generic Routing Encapsulation) multipoint. This is required for DMVPN to allow multiple spokes to communicate with each other through the hub.
	tunnel key 10000Y	Sets the key for the GRE tunnel, which is used to differentiate between different GRE tunnels.
EIGRP	router eigrp AS_NUM	Starts the EIGRP (Enhanced Interior Gateway Routing Protocol) process with Autonomous System (AS) number AS_NUM.
	network 192.168.1.X 0.0.0.0	Advertises the 192.168.1.X/32 network in EIGRP.
	network 10.0.0.0 0.255.255.255	Advertises the 10.0.0.0 network in EIGRP.
	no auto-summary	Disables automatic summarization of networks at major network boundaries.

## Part 4 –NAT

step	Command or Action Purpose	Purpose
NAT	Interface outside_interface	This command specifies the interface on the router that connects to the outside network (typically the internet). You would replace <code>outside_interface</code> with the actual name of the interface, such as <code>GigabitEthernet0/0</code> .
	Ip nat outside	This command designates the specified interface as the outside interface for NAT. Traffic that comes in or goes out of this interface will be subject to NAT.
	Interface inside_interface	This command specifies the interface on the router that connects to the inside network (typically the local area network or LAN). You would replace <code>inside_interface</code> with the actual name of the interface, such as <code>GigabitEthernet0/1</code> .
	Ip nat inside	This command designates the specified interface as the inside interface for NAT. Traffic that comes in or goes out of this interface will be subject to NAT.
	Ip nat inside source list 1 interface outside_interface overload	This command configures NAT to use a list of IP addresses (specified by access list 1) and translate them to the IP address of the specified outside interface, allowing multiple inside addresses to share the same public IP address using port address translation (PAT). The <code>overload</code> keyword indicates that PAT is being used, which allows multiple devices to share a single public IP address by using different ports.
	Access-list 1 permit any	This command creates an access control list (ACL) with the number 1 and allows all IP traffic. The <code>permit any</code> part of the command means that all IP addresses are permitted by this ACL.

## Part 5 – IPSEC

step	Command or Action Purpose	Purpose
Encryption properties	crypto isakmp policy 10	This command defines an ISAKMP policy with priority number 10. ISAKMP policies determine the parameters used during the negotiation of the ISAKMP security association (SA).
	hash md5	Specifies the hash algorithm to use for the policy. MD5 (Message Digest Algorithm 5) is used to ensure data integrity.

# DMVPN LAB

	authentication pre-share	Sets the authentication method to pre-shared keys. Pre-shared keys are a method where both parties use the same shared secret key for authentication.
	encryption 3des	Defines the encryption algorithm to use, which in this case is 3DES (Triple Data Encryption Standard). 3DES encrypts data three times for enhanced security.
	group 2	Specifies the Diffie-Hellman group to use for key exchange. Group 2 corresponds to a 1024-bit key, which provides a balance between security and computational efficiency.
	lifetime 86400	Sets the lifetime of the ISAKMP security association to 86400 seconds (24 hours). This means the SA will need to be re-negotiated every 24 hours.
Encryption key	crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0	Defines a pre-shared key ( <code>cisco123</code> ) for ISAKMP with a wildcard address ( <code>0.0.0.0 0.0.0.0</code> ). This means the pre-shared key can be used for any IP address.
Transform set	crypto ipsec transform-set myset esp-3des esp-md5-hmac	Creates an IPsec transform set named <code>myset</code> . A transform set defines how the IPsec traffic will be protected: <ul style="list-style-type: none"> <li><code>esp-3des</code> specifies the use of 3DES for encryption.</li> <li><code>esp-md5-hmac</code> specifies the use of MD5 for integrity and authentication.</li> </ul>
	mode transport	Sets the IPsec mode to transport mode, where only the payload of the IP packet is encrypted and/or authenticated.
IPSEC profile	crypto ipsec profile cisco	Creates an IPsec profile named <code>cisco</code> . An IPsec profile is a set of IPsec parameters that can be applied to interfaces or tunnels.
	set transform-set myset	Associates the transform set <code>myset</code> with the IPsec profile <code>cisco</code> .
	set security-association lifetime seconds 86400	Sets the security association (SA) lifetime to 86400 seconds (24 hours) for the IPsec profile. This means the IPsec SA will need to be re-negotiated every 24 hours.
	set security-association lifetime kilobytes 4608000	Sets the SA lifetime to 4608000 kilobytes. This means the IPsec SA will need to be re-negotiated after transferring 4608000 kilobytes of data.
Reference GRE tunnel to the encryption	tunnel protection ipsec profile cisco	Applies the IPsec profile <code>cisco</code> to the tunnel interface, providing IPsec protection to the traffic passing through the tunnel.